Amendments to the claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for monitoring of communications traffic, comprising:

connecting a recorder to a network switch to record packet-data communication traffic received from, and passing through, the network switch;

encrypting the packet-data communication traffic at an encryption engine communicatively connected to the recorder after the packet-data communication traffic has passed through the network switch to create encrypted data; and

storing the encrypted data in a storage device such that the encrypted data can be decrypted only by means of decryption keys that exhibit restricted availability, wherein encrypted search conditions are included within the decryption keys.

2. (previously presented) The method as claimed in Claim 1 further including employment of a spare disk and/or CPU capacity within a telecommunications system.

3. (canceled)

4. (previously presented) The method as claimed in Claim 1, further including the step of employing separate levels of authorization for access to the stored data.

5. (previously presented) The method as claimed in Claim 1, further including the step of employing a decryption key that is useable only once.

6. (previously presented) The method as claimed in Claim 1, further including the step of logging all accesses to the stored data to an encrypted secure audit trail.

7. (previously presented) The method as claimed in Claim 1, further including a tamper detection reference within the encrypted data.

8. (previously presented) The method as claimed in Claim 1, further including the step of monitoring all the available communications traffic.

9. (previously presented) The method as claimed in Claim 8, wherein the step of storing the recorded traffic comprises the step of recording all of the recorded traffic.

10. (previously presented) The method as claimed in Claim 1, wherein the communications traffic to be recorded comprises traffic through a telecommunications switch, router or gateway.

11. (previously presented) The method as claimed in Claim 1, further including the step of encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access.

12. (previously presented) The method as claimed in Claim 1. further including the step of authorizing use of the required decryption key in a restricted manner.

13. (currently amended) A system for monitoring of communications traffic, comprising:

a recorder that records the communications traffic, the communications traffic being received by the recorder from a network switch;

an encryption engine that encrypts the communications traffic after the communications traffic has passed through the network switch to the recorder; and

a storage device that stores recorded communications traffic as encrypted data, such that the encrypted data can be decrypted only by means of keys that exhibit restricted availability, wherein encrypted search conditions are included within the keys.

14. (previously presented) The system as claimed in Claim 13 further including application software that executes the method steps of anyone or more of Claims 2-12.

15. (canceled)

16. (canceled)

17. (previously presented) A method for monitoring of communications traffic, comprising the steps of:

receiving communications traffic from a network switch at a recorder;

encrypting the communications traffic after the packet-data communication traffic has passed through the network switch to the recorder in order to generate encrypted communications traffic data;

storing the encrypted communications traffic data in a storage device such that the encrypted communications traffic data can be decrypted by decryption keys that exhibit restricted availability, that allow encrypted search conditions, and that employ separate levels of authorization for access to the stored data; and

encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access.

18. (previously presented) The method as claimed in Claim 17, further including the step of employing a decryption key that is useable only once.

19. (previously presented) The method as claimed in Claim 17, further including the step of logging all accesses to the stored data to an encrypted secure audit trail.

20. (previously presented) The method as claimed in Claim 17, further including a tamper detection reference within the encrypted data.

21. (previously presented) The method as claimed in Claim 17, further including the step of monitoring all the available communications traffic.

22. (previously presented) The method as claimed in Claim 17, wherein the step of storing the recorded traffic comprises the step of recording all of the recorded traffic.